IN THE CLAIMS

Please amend the claims as follows:

Claim 1-14 (Canceled).

Claim 15 (Currently Amended): A system for protecting a communication device against a denial-of-service attack, the system comprising:

a monitoring device provided on a local area network including the communication device, the monitoring device being configured to monitor a packet transmitted to the communication device via an internet-service-provider network; and

a restricting device provided on the internet-service-provider network, the restricting device being configured to restrict a packet to the local area network,

wherein the monitoring device includes

an attack detecting unit configured to detect an attack by the packet on the communication device, and

a protection-request-information transmitting unit configured to transmit to the restricting device protection request information indicating a request for protection against the attack, the protection request information including a certificate authenticating the monitoring device, the protection-request-information transmitting unit being configured to update the protection request information to remove ~~exclude from restriction~~ packets not included in the attack from restriction [[,]] based on a report of received packets transmitted from the restricting device, and

the restricting device includes a packet restricting unit configured to restrict a packet transmitted to the communication device via the internet-service-provider network based on the protection request information.

Claim 16 (Previously Presented): The system according to claim 15, wherein

the monitoring device further includes a signature generating unit configured to generate a signature indicating a feature of a packet that attacks the communication device,

the protection-request-information transmitting unit transmits the protection request information including the signature to the restricting device, and

the packet restricting unit restricts a packet corresponding to the signature.

Claim 17 (Previously Presented): The system according to claim 16, wherein

the restricting device further includes a signature determining unit configured to determine whether the protection request information including the signature is appropriate based on the certificate, and

the packet restricting unit restricts a packet corresponding to a signature determined to be appropriate, and does not restrict a packet corresponding to a signature determined to be inappropriate.

Claim 18 (Previously Presented): The system according to claim 16, wherein

the restricting device further includes

a report generating unit configured to generate a report including a feature and an amount of packets corresponding to the signature, and a report transmitting unit configured to transmit the report to the monitoring device,

the signature generating unit generates a new signature based on the report,

the protection-request-information transmitting unit transmits the protection request information including the new signature to the restricting device, and

the packet restricting unit restricts a packet corresponding to the new signature.

Claim 19 (Previously Presented): The system according to claim 18, wherein the restricting device further includes a forwarding unit configured to forward the protection request information to other restricting devices provided on the internet-service-provider network, the forwarding unit being configured to determine whether to forward the protection request information based on the report generated by the report generating unit.

Claim 20 (Previously Presented): The system according to claim 17, wherein the restricting device further includes a determination-result transmitting unit configured to transmit a determination result of the signature determining unit to the monitoring device, the signature generating unit of the monitoring device generating a new signature indicating the feature of the packet that attacks the communication device when the determination result indicates that the signature is inappropriate.

Claim 21 (Currently Amended): A method of causing a monitoring device and a restricting device to protect a communication device against a denial-of-service attack, the monitoring device being provided on a local area network including the communication device and being configured to monitor a packet transmitted to the communication device via an internet-service-provider network, the restricting device being provided on the internet-service-provider network and being configured to restrict a packet to the local area network, the method comprising:

detecting, at the monitoring device, an attack by the packet on the communication device;

transmitting, from the monitoring device to the restricting device, a protection request information indicating a request for protection against the attack, the protection request information including a certificate authenticating the monitoring device;

restricting, at the restricting device, packets transmitted to the communication device via the internet-service-provider network based on the protection request information;

transmitting, from the restricting device to the monitoring device, a report including information on packets included the attack; and

transmitting, from the monitoring device to the restricting device, an updated protection request information removing ~~excluding from restriction~~ packets not included in the attack from restriction [[,]] based on the report.

Claim 22 (Previously Presented): The method according to claim 21, further comprising:

generating, at the monitoring device, a signature indicating a feature of a packet that attacks the communication device, wherein

protection request information transmitted to the restricting device includes the signature, and

a packet corresponding to the signature is restricted.

Claim 23 (Previously Presented): The method according to claim 22, further comprising:

determining, at the restricting device, whether the protection request information including the signature is appropriate based on the certificate,

wherein a packet corresponding to a signature determined to be appropriate is restricted, and a packet corresponding to a signature determined to be inappropriate is not restricted.

Claim 24 (Previously Presented): The method according to claim 22, further comprising:

generating, at the restricting device, a report on a feature and an amount of packets corresponding to the signature; and

transmitting the report from the restricting device to the monitoring device,

wherein a new signature is generated at the monitoring device based on the report, protection request information including the new signature is transmitted to the restricting device, and a packet corresponding to the new signature is restricted.

Claim 25 (Currently Amended): A non-transitory computer-readable medium storing thereon computer-readable instructions for protecting a communication device against a denial-of-service attack using a monitoring device and a restricting device, the monitoring device being provided on a local area network including the communication device and being configured to monitor a packet transmitted to the communication device via an internet-service-provider network, the restricting device being provided on the internet-service-provider network and being configured to restrict a packet to the local area network, the computer-readable instructions when executed by a computer cause the computer to perform the method comprising:

detecting, at the monitoring device, an attack by the packet on the communication device;

transmitting, from the monitoring device to the restricting device, protection request information indicating a request for protection against the attack, the protection request information including a certificate authenticating the monitoring device;

restricting, at the restricting device, a packet transmitted to the communication device via the internet-service-provider network based on the protection request information;

transmitting, from the restricting device to the monitoring device, a report including information on packets included the attack; and

transmitting, from the monitoring device to the restricting device, an updated protection request information removing ~~excluding from restriction~~ packets not included in the attack from restriction [[,]] based on the report.

Claim 26 (Currently Amended): The non-transitory computer-readable medium according to claim 25, further comprising:

generating, at the monitoring device, a signature indicating a feature of a packet that attacks the communication device;

transmitting, from the monitoring device to the restricting device, the protection request information including the signature; and

restricting, at the restricting device, a packet corresponding to the signature.

Claim 27 (Currently Amended): The non-transitory computer-readable medium according to claim 26, further comprising:

determining, at the restricting device, whether the protection request information including the signature is appropriate based on the certificate;

restricting a packet corresponding to a signature determined to be appropriate; and

not restricting a packet corresponding to a signature determined to be inappropriate.

Claim 28 (Currently Amended): The non-transitory computer-readable medium according to claim 26, further comprising:

generating, at the restricting device, a report on a feature and an amount of packets corresponding to the signature; and

transmitting the report from the restricting device to the monitoring device;

generating, at the monitoring device, a new signature based on the report;

transmitting, from the monitoring device to the restricting device, the protection request information including the new signature; and

restricting, at the restricting device, a packet corresponding to the new signature.